HACKERS

Seguridad en la Red

By Jacktu

Introducción.-

Desde que los ordenadores forman parte de mi vida cotidiana, al igual que en la mayoría de los hogares de hoy en día, la Seguridad y el control de mis Documentos siempre ha sido una obsesión. El tener todos esos documentos a salvo de mirones y curiosos no es una labor difícil ni que lleve mucho tiempo; simplemente tener un poco de cuidado y esmero en la configuración y control del sistema. Normalmente pensaremos que quien va a entrar en mi ordenador si no tengo nada de interés; efectivamente, un hacker no creo que esté interesado en ese tipo de ordenadores, salvo que busque algo en concreto. Pero hoy día circula por Internet numerosa información, manuales, etc. sobre técnicas de hacking y cualquier persona puede, con unos medios y conocimientos mínimos, lanzarnos un ataque.

Hay que distinguir entre Hacker, Cracker y Pirata. Normalmente todo el mundo cree que es lo mismo cuando evidentemente tienen un significado totalmente distinto. Un hacker es aquella persona que le interesa enormemente la informática y que tiene unas grandes ansias de aprender cada vez más y estudiar los sistemas. Evidentemente estudia sus fallos, violando normalmente dichos sistemas. El hacker no destruye, simplemente entra en un sistema, ve sus fallos y se va (no sin antes dejar su huella). Un hacker, antes de lanzar un ataque, estudia meticulosamente el sistema objeto de ese ataque, puede tardar incluso meses en estudiarlo; los únicos ficheros que puede modificar, en un sistema, un hacker son aquellos imprescindibles para borrar sus huellas. El cracker por el contrario “rompe” y “destruye”; el cracker puede borrar ficheros, destruir sistemas, romper claves de seguridad y passwords, introducen virus, etc. No obstante, yo opino que en numerosas ocasiones un hacker también utiliza técnicas cracker, por ejemplo cuando tienen que romper un password para poder penetrar en un sistema. El pirata es aquel que se dedica a copiar sofware legal y protegido persiguiendo una remuneración económica o cualquier otra forma de lucro. También podemos decir que pirata es por ejemplo el que entra en un sistema con el objeto de “robar” una lista de tarjetas de crédito o cualquier otro tipo de dato que posteriormente va a poder vender y obtener un beneficio económico.

Por último, tampoco nos podemos olvidar de los “lámer” (aquellas personas que se creen que tienen algún conocimiento informático y lo único que hacen es utilizar numerosos sploit y programas que abundan en la Red y que utilizan para atacar sistemas, normalmente pequeños ordenadores de usuarios normales y caseros). Esta gente en realidad carece de los más mínimos conocimientos y simplemente se pueden dedicar a utilizar los programas creados por verdaderos hackers. Evidentemente, a mi entender, para los usuarios caseros son ésta gente la más peligrosa, ya que utilizando un simple sploit pueden dañar, robar, modificar, etc. nuestra información del disco duro y suelen ser gente joven que no tiene conciencia real del daño que pueden causar. Digo que para nosotros pueden ser los más peligrosos ya que estas personas no son capaces de entrar en auténticos sistemas protegidos, por lo que tienen que optar por ordenadores personales de los cuales, por ejemplo, han obtenido previamente la IP en cualquier IRC.

Todo esto no quiere decir que solamente podamos recibir un ataque o una entrada ilegal en nuestra máquina por parte de estos pequeños “lámer”. Podemos recibir un ataque en cualquier momento, desde cualquier lugar y efectuado por cualquier hacker, cracker o lámer.

Tampoco nos debemos confundir un nubbie con un lámer; el lámer, como ya he dicho anteriormente es la persona que no tiene prácticamente conocimiento alguno de informática por lo que se tiene que contentar con utilizar medios realizados por otras personas (hacker o cracker) para poder sorprender a amigos y conocidos. El nubbie por el contrario es la persona realmente interesada en estos temas y que tiene intención y voluntad de aprender. Lo que pasa que, claro está, nadie ha nacido aprendido, por lo que este gente necesita un período de aprendizaje y alguien que le enseñe.

También os preguntareis como es posible que un lámer sea a la vez nuestra peor pesadilla y a la vez diga que no tiene ni idea de informática. Muy sencillo, pues por que para hackear no hace falta grandes conocimientos ni grandes sistemas informáticos. Hackear es muy sencillo y cualquiera puede hacerlo (puede hasta un lámer.. ;-) otra cosa muy distinta es entrar en grandes sistemas, eso es lo que yo llamo auténtico hackeo)

La siguiente pregunta que os haréis es ¿es entonces mi Güindos seguro o no es seguro? Pues lamentablemente tengo que decirte que NO, tu Güindos no es para nada seguro. Otra cosa muy distinta es pensar que como no es seguro pues no tengo que preocuparme de nada, ya que por mucho que lo intento no voy a conseguir nada. Una cosa es que tu sistema no sea seguro y otra muy distinta es facilitar más aún las cosas a los hacker (o lámer).

Poniendo un poco de cuidado y teniendo unas básicas y elementales medidas de seguridad podemos obtener un nivel más que aceptable de nuestro sistema. Pero nunca, digo nunca, penséis que teneis un sistema 100 % seguro ya que eso en Güindos es imposible; digamos que tendremos que volvernos un poco paranoicos al objeto de obtener ese nivel aceptable de seguridad.

Con estas pequeñas normas que a continuación voy a citar, creo que podéis llegar a tener ese nivel deseado. No obstante si encontráis algún error o tenéis alguna duda, por favor, mandarme un mail a la siguiente dirección**: jacktu2000@mixmail.com** prometo que contestaré todos los mail que me remitáis.

Jacktu

jacktu2000@mixmail.com

Conceptos y definiciones básicas.-

En primer lugar vamos a definir y conocer unos conceptos básicos. Más que definir y conocer debería decir repasar, ya que creo que son conceptos que hoy día conoce todo el mundo.

Las Redes podemos decir que son varios ordenadores conectados entre si. Dentro de las redes podemos encontrar una red local (red Lan), que sería por ejemplo tu ordenador de la sala y el ordenador de la habitación conectados entre si y, una red internet que sería tu ordenador conectado a internet a través de tu proveedor. Para que todos estos ordenadores se entiendan entre si y puedan intercambiar información, necesitan unos protocolos (TCP) e identificarse entre si. Para identificarse entre si utilizan las **IP**; esta IP es importantísima ya que para iniciar un ataque a nuestra máquina, necesitan saber cual es nuestra IP por lo que es algo importante de proteger y ocultar. Las IP tienes el formato siguiente: XXX.XXX.XXX.XXX donde XXX es un número comprendido entre o y 255. Nunca se podrá superara ese número 255. Unos ejemplos de Ips válidas podrían ser 213.55.666.12, hay que tener en cuenta que no tiene que ser necesariamente grupos XXX también puede ser XX o incluso X, pero sin perder la norma de que cada grupo no puede superar el 255. Estas IP pueden ser dinámicas o estáticas; decimos que son estáticas cuando siempre tenemos la misma IP (como por ejemplo ADSL, Cable, etc.) y decimos que son dinámicas cuando cada vez que nos conectamos a la Red, se nos asigna una IP distinta (Tarifa plana normal, conexión gratuita, conexión normal, etc.). Queda evidente que el principal peligro de una ADSL o cable sería el poseer una IP estática (y su principal ventaja sería el ancho de banda, claro). ¿Como puedo saber cual es mi IP? Muy sencillo, según el sistema operativo que tengas. Si tienes Win95 ó Win98 pulsa inicio-programas-Ms-dos y se abrirá una ventana de Ms-Dos (el Ms-Dos es uno de los primeros sistemas operativos de Mocosoft). Actualmente los sistemas Win95, Win98 y WinMe se basan y apoyan en el Ms-Dos, de ahí su inestabilidad y peligro. Si tu sistema es WinMe el Ms-Dos está camuflado por lo que tienes que ir a Inicio-ejecutar y teclear “Command.com” (sin las comillas claro :-P). Una vez tecleado esto y tras pulsar enter nos aparecerá una pantalla de Ms-Dos. Si esta pantalla no aparece en una ventana (me refiero si aparece a pantalla completa) pulsar ALT+ENTER. Si estamos a pantalla completa y queremos volver a win simplemente tenemos que teclear “Exit”. Bien, ahora ya estamos en una pantalla de Dos, ahora simplemente tecleamos la orden “ipconfig” y nos aparecerá nuestra IP.

Llamamos **Puertos** por donde entra y sale la información, esto es una forma un poco bruta de definición pero es para que se entienda mejor. Por ejemplo, el puerto por el que nos llega el correo MSTP es el 25, el puerto por el que se comunica la impresora al ordenador es el puerto paralelo o puerto USB, el puerto que utilizaría el NetBios utilizando el protocolo TCP IP sería el puerto 139. Solamente decir que hay unos 65.000 puertos.

El **Protocolo** es el conjunto de normas, reglas, leyes, formalidades, etc. que los ordenadores utilizan para su comunicación con otros ordenadores. **NetBios** es el protocolo para compartir archivos e impresoras (se puede compartir archivos, impresoras o archivos e impresoras).

Tras este pequeño repaso (no quiero cansar con más definiciones, en lo sucesivo iré explicándolas según vayan apareciendo nuevos términos los cuales crea que pueden no ser

conocidos por los lectores) pasamos inmediatamente a lo que realmente nos interesa saber y es las técnicas y métodos para defender la información que hay en el disco rígido de nuestra máquina así como controlar que programas acceden o se comunican con nuestro ordenador al objeto de evitar cualquier intruso.

Instalación del Sistema.-

En primer lugar vamos a partir de cero, por lo que comenzamos por la instalación de Güindos. Cuando instalamos Güindos, el sistema nos pregunta en que directorio lo queremos instalar. Por defecto nos muestra y aconseja que lo instalamos sobre el directorio C:/windows. Bien, pues aquí ya tenemos el primer parámetro que podemos cambiar al objeto de que si posteriormente nuestro sistema es atacado por un virus el cual busca normalmente este directorio para infectar (no todos funcionan así, claro) no lo encuentre con lo que evidentemente no conseguirá infectarnos.

Siguiendo con la instalación y configuración del sistema, también podemos deshabilitar una opción que normalmente, viene habilitada por defecto. La opción que debemos deshabilitar es la opción “ocultar las extensiones para tipos conocidos de archivo”. Con esta opción habilitada lo que ocurre es que no vemos las extensiones de los ficheros conocidos, por lo que puede pasar que nos metan un fichero ejecutable (*.exe, *.com, *.bat) diciéndonos por ejemplo que se trata de una fotografía, cuando evidentemente una fotografía no puede tener estas extensiones ya que son otras las que puede tener (*.bmp, *.jpg, *.gif, *.pcx, etc.). Sobre los tipos de extensiones de los ficheros, hablaremos extendidamente más tarde. Para desactivar la opción “ocultar las extensiones para tipos conocidos de archivo” nos iremos a Explorador de Windows-Herramientas-opciones de carpeta-pestaña “ver”-deshabilitamos dicha opción.

Otra de las opciones que se debe tener en cuenta es el “NetBios”. Como dijimos anteriormente NetBios lo utilizamos para compartir archivos e impresoras. Esta opción la tendremos deshabilitada si no es totalmente necesario. Para habilitar o deshabilitar esta opción iremos a MiPc-Panel de control-Red-Pestaña “configuración” compartir archivos e impresoras. Si tenemos que habilitar esta opción por necesidad, la pondremos con contraseña para dificultar el acceso indeseado por ese puerto. Para poner contraseña ir a MiPc-Panel de control-Red-Pestaña Control de Acceso.

Pese a que pongamos contraseña no quiere decir que estemos totalmente cubiertos; como demostraré más adelante las contraseñas de Güindos y de muchiiiiiiiisimos programas, son fácilmente violables.

Más sobre IPs y NetBios.-

Como hemos dicho anteriormente nuestra IP es algo muy importante, por lo que la

debemos ocultar y proteger. Numerosas veces al ir navegando por la Red, vamos dejando reflejada en diversos registros nuestra IP. Claro está que tampoco nos vamos a volver unos paranoicos con proteger y ocultar la IP, ya que no vamos a hacer nada ilegal. Pese a todo si

queremos navegar en el anonimato podemos hacerlo de diferentes forma.

Podemos utilizar el servicio "Anonymizer", este servicio se contrata en http://www.anonymizer.com. En este servicio podemos pagar por él o utilizarlo gratis. Si lo utilizamos gratis tendremos alguna limitación (no hay acceso a HTTPS ni FTP) solo da acceso a HTTP y además con un retardo de unos 30 segundos. Al utilizar este servicio la IP que quedaría en el registro de la página o sitio que visitemos no sería la nuestra si no la de Anonymizer. (Ojo con los avispados, si quieres utilizar este servicio para realizar algo ilegal, evidentemente nadie conocerá tu IP, ya que quedará reflejada la de Anonymizer, pero Anonymizer SI que conoce cual es tu IP).

Otra forma de ocultar tu IP es utilizando un Proxy. Esto es parecido al servicio Anonymizer ya que accedemos a las páginas por medio de un Proxy en vez de acceder directamente nosotros. Yo personalmente no recomiendo el uso de proxy ya que reduce enormemente la navegación y no todos son realmente anónimos. Por estos motivos no me extiendo más sobre esta forma de ocultación.

Donde, yo personalmente creo, que se debe guardar la información de la IP es cuando se utiliza un Chat, mensajería instantánea (como Messenger o Yahoo), etc. ya que ahí es donde realmente nos la puede pillar el dichoso lámer. ¿Como nos la puede pillar? Pues muy sencillo, vamos a ver alguna forma como ejemplo.

Imaginemos que estamos en una sesión de Messenger y queremos saber la IP de un contacto pues lo único que tenemos que hacer es abrir una ventana de ms-dos (como explicamos anteriormente) y una vez que la tengamos abierta le mandamos cualquier fichero a esa persona por el messenger (le podemos mandar por ejemplo cualquier texto que sea grande al objeto de tener tiempo para teclear una orden en la ventana de ms-dos); mientras ese fichero se está transfiriendo en la ventana de ms-dos tecleamos la orden "netstat -a" (recordar que no se ponen las comillas) y seguidamente en esa misma pantalla de ms-dos nos aparecerá la IP de esa persona. Si por el contrario nos encontramos en una sesión de IRC simplemente tenemos que teclear en dicha sesión "/dns nick" (donde nick pondremos el nick que utilice en ese momento dicha persona) y aparecerá su IP. Fácil ¿eh? Yo por eso no utilizo el IRC y mediante el messenger Yahoo y Messenger de Hotmail solo me comunico con gente conocida.

Otra forma de pillarnos la IP es por medio de los e-mail. Cuando recibimos un e-mail picamos con el botón derecho sobre él y nos vamos a "Propiedades", seguidamente picamos en la solapa "Detalles" y, normalmente en la primera línea que aparece donde pone "Received: from XXX.XXX.XXX.XXX" donde las X son los números de la IP del remitente.

Si en la ventana de ms-dos tecleamos la orden netstat IP, donde IP sería la Ip de la máquina que queremos explorar, nos dará en pantalla una relación detallada de los puertos que tiene abiertos y en conexión; puedes hacer una prueba introduciendo la orden netstat Ip donde IP

en este caso pondremos la nuestra y así sabremos que puertos tenemos abiertos. En este caso también nos valdrá la formula “netstat localhost” que nos dará también los puertos que tiene nuestra máquina abierta ya que “localhost” equivale a nuestra IP.

Ya sabemos que es NetBios y como podemos protegerlo, ahora vamos a ver como podríamos recibir un ataque por dicho puerto.

Supongamos que tenemos la IP de una máquina y queremos saber si esta máquina se encuentra conectada en este momento. En una ventana de ms-dos tecleamos Ping Ip (donde Ip pondremos la de la máquina que queremos atacar). En la relación que nos aparecerá seguidamente, al final si pone por ejemplo <0% perdidos> quiere decir que esa máquina se encuentra conectada, si al final pone <100% perdidos> quiere decir que se encuentra desconectada. Vamos a suponer que nos ha dado <0% perdidos>; ya sabemos que esa máquina está conectada. Lo siguiente que nos interesa es saber si tiene NetBios abierto y si comparte ficheros o impresoras. Para ello tecleamos nbtstat -a IP (ojo, la orden ya no es la de antes, fijarse bien), donde como de costumbre la IP es la de la máquina donde vamos a entrar. Seguidamente nos aparecerá un cuadro con diversa información como nombre, tipo y estado en tipo aparecerán unos números (eso es lo que nos interesa) si aparece <20> eso es que tiene ficheros o impresoras compartidos. Seguidamente tecleamos “net view //IP” y nos aparecerá más información de esos recursos compartidos. Si queremos ver esos recursos como si estuviésemos en ese disco duro y manejarlos como si del nuestro se tratase lo único que nos resta hacer es abrir el explorador de Güindos (I.E.) y donde ponemos las direcciones de las web a las que queremos acceder pondremos en este caso “//IP/nombrerecurso (donde nombre recurso será el que nos aparezca en el resultado de la opción “net view //IP (por ejemplo //134.165.65.34/Documentos c). Acabamos de descubrir un importante bug (agujero de seguridad) en el programa Internet Explorer de Microsoft. Este agujero consiste en que dicho programa es un shell esto quiere decir que se puede utilizar como se utiliza normalmente el Explorador de Windows (teclea ahora donde ponemos las direcciones web, simplemente C: y pulsa Enter, voila aquí tienes las carpetas de tu disco duro).

Con estos ejemplos quiero que veáis lo importante que resulta no tener recursos compartidos y, si realmente tenemos que tenerlos, éstos hay que ponerlos bajo una contraseña (aunque ya se verá que no son del todo seguras en esto de Güindos).

Contraseñas.-

Como ya he dicho anteriormente, las contraseñas no son del todo fiables y cualquier persona con unos pocos conocimientos podría fácilmente saltarlas. A modo de ejemplo decir que yo, simple aficionado a la informática, al saltar contraseñas en documentos de Officce las he llegado a saltar en menos de tres segundos. ¿Que no será capaz de hacer un auténtico guru de la Informática?

A la hora de elegir una contraseña, debemos complicarla todo lo posible. Esto quiere decir que NUNCA debemos poner nombre conocidos o que fácilmente figuren en los diccionarios, ya que empleando numerosos programas que hay en internet, éstos mediante

diccionarios nos la pueden encontrar fácilmente. El funcionamiento de estos programas es sencillo, vamos a poner por ejemplo el programa “Brutus”; lo que hace este programa es coger unos diccionarios e ir probando posibles contraseñas que figura en dichos diccionarios hasta encontrar la correcta (esta forma se denomina Brute Forcing). También hay diversos programas para saltar passwords

concretos como por ejemplo los creados con el Officce (como por ejemplo el programa Advanced Office 2000 Password Recovery).

Así mismo Güindos guarda las contraseñas de inicio de sesión, de internet, etc. en un fichero que tiene por nombre el que hayas marcado tu al instalar el windows y como extensión tiene PWL. Si por cualquier motivo (te han pedido ese fichero, engañándote o por cualquier otro medio) alguien se hace con ese fichero tendrá todos tus passwords. Este fichero lo pueden visionar con diversos programas como por ejemplo “Pass Word List” o el “PWL-Hacker”.

Una forma de que este fichero no tenga estos password sería teclear tu siempre las contraseñas, nunca indicar que windows recuerde la contraseña para no tenerla que teclear por ejemplo cada vez que entras en internet (fíjate cuando entres en internet y donde tienes que poner la contraseña hay un cuadradito que si lo marcas windows recordará la misma, este cuadradito siempre tiene que estar en blanco y así marcar tu la contraseña cada vez que te conectes). Hay formas también de saltarse la contraseña de sesión de windows, de los protectores de pantalla, etc, pero como para esto se supone que el supuesto hacker tiene que tener acceso físico a tu ordenador, no nos vamos a parar en este tema, ya que por el momento lo que nos interesa es protegernos del acceso a nuestro ordenador vía Internet. Decir también que en sistemas Windows XP y en windows NT los ficheros de las contraseñas se guardan en “windows/system32/config con el nombre “sam.log”.

Una contraseña que dificultaría el acceso (digo dificultaría, ya que evidentemente siempre podrá ser reventada) sería por ejemplo a&bv55%%MB. Como podéis comprobar utilizamos letras mayúsculas, minúsculas, números y símbolos con el objeto de que ésta no pueda ser violada por medio de diccionarios (repito que esto no quiere decir que no existan programas que las salten, como el mencionado para saltar contraseñas de Officce) lo que pasa que le dificultaríamos el trabajo al hacker (con un poco de suerte se cansa y lo deja). También sería una buena política el cambiar frecuentemente de contraseña (por ejemplo cada 15 o 30 días).

Las Cookies y el Spyware.-

Aquí tenemos otras dos formas de que nos controlen por Internet. Las Cookies son unos pequeños ficheros (se almacenan en c:/windows/cookies y se pueden borrar tranquilamente después de cada sesión de internet) los cuales muchas veces son necesarios para visualizar correctamente una web, indicando si el usuario está o no conectado. Ten en cuenta que uno de los datos que puede enviar es tu IP.

Es Spyware son ficheros normalmente introducidos ocultamente en programas freeware

(gratuitos) que envían información sobre hábitos del usuario (que páginas consulta, etc.), también puede mandar la IP de la máquina. ¿como podemos solucionar esto? Pues muy sencillo:

En relación con las cookies se puede configurar el navegador para deshabilitar las mismas y así que no se almacenen en nuestro disco duro. Pare ello iremos a Herramientas-opciones internet-pestaña de seguridad-nivel de seguridad de la zona-lo subimos a nivel alto. También

podríamos ir a personalizar nivel y desde ahí acceder a más opciones y deshabilitar controles actives, java, etc. Hay que tener en cuenta que si deshabilitamos las cookies, los controles actives, java, etc. puede ocurrir que alguna web no la visualicemos correctamente. Yo personalmente prefiero eliminar manualmente las cookies cada vez que termino una sesión en Internet.

Para el caso del Spyware, lo tenemos más fácil. Recomiendo el programa gratuito "Ad-Ware" el cual nos limpia perfectamente el disco duro de todos estos ficheros. En este caso hay que tener en cuenta que si eliminamos esos ficheros espía, el programa en el cual venían puede no funcionar correctamente o no funcionar en absoluto. Fijémonos que normalmente vienen en programas gratuitos y actualmente ya no hay tanta avalancha como antes. Yo prefiero quedarme sin el programa en el cual vienen esos ficheros que tenerlo instalado y me estén espiando continuamente.

La mayoría de los usuarios tenemos instalados en los scripts algún tipo de add-on que automatizan las tareas (envió de sms, etc.), pues aquí tenemos otro apartado potencialmente peligroso ya que aquí SI nos pueden meter Código malicioso. Se podrían editar antes de instalarlo, pero sinceramente hay que tener algún conocimiento de programación para ver si nos han colado algún código malicioso. Por tanto no me extiendo más sobre este tema.

Tipos de archivos.-

Es importantísimo conocer las extensiones más usuales que nos podemos encontrar en el sistema, para saber ante que tipo de fichero nos encontramos. Es muy usual por ejemplo que en el IRC o cualquier otro programa de mensajería instantánea (messenger de hotmail, messenger de Yahoo, etc.) nos engañen y nos digan que nos mandan un fichero, por ejemplo de una foto y nosotros lo recibimos y ejecutamos para verla y en realidad lo que nos han mandado en un sploit (fichero ejecutable con código malicioso que lo que hace es aprovechar algún agujero en concreto para acceder a nuestro ordenador o quitarnos una cuenta de correo, etc.). Pues para saber esto nada más lejos que conocer las extensiones de los ficheros.

Los ficheros peligrosos (y que nunca debemos aceptar salvo que sea de gente de confianza) tienen extensiones *.exe, *.com y *.bat (el asterisco sería cualquier nombre). Algunas de las extensiones de fotografía serían *.jpg, *.gif (estas dos en Internet son las más utilizadas por el sistema de compresión que utilizan y que ocupan muy poco espacio), *.bmp, *.pcx, *.pds, los que tienen extensión *.txt son de texto así como los *doc. y otras similares que utilizan determinados procesadores de texto;*.ini son de inicio (ejemplo win.ini), *.dat contienen datos, *.bin (binarios), *.html o *.htm son de páginas web y así podríamos seguir en una interminable

lista. Lo más importante es diferenciar cuando se trata de un fichero ejecutable ya que realmente es ahí donde podemos tener un peligro potencial.

Ingeniería Social.-

La ingeniería social es un concepto sencillo de definir. Es ni más ni menos que el engaño. ¿A que me refiero con esto? Pues muy sencillo, vamos a poner un ejemplo; imaginaos que consigo cierto nivel de confianza con vosotros y de buenas a primeras, un día le digo a cualquier contacto, con el que previamente he cogido confianza, que tengo un archivo en mi ordenador que lo he borrado sin querer y que debido a ello mi máquina se cuelga. Seguidamente le digo que el archivo en cuestión tiene la extensión *.pwl si por favor me puede pasar el de su ordenador para solucionar mi problema.

Estaría casi seguro que el 90 % de la gente a la que se lo pidiese no pondría pega alguna en darme una copia. Como recordareis me esta pasando el fichero *.pwl con lo que también me está pasando todas las contraseñas de su equipo. Esto es a grandes rasgos lo que es la Ingeniería social y os aseguro que se consiguen muchísimos datos utilizándola.

Firewalls.-

Una buena opción que debemos tener para controlar los niveles de seguridad de nuestra máquina es instalar un firewalls o cortafuego. La función de este programa es sencilla, controla y monitoriza todos los accesos y transferencias de nuestro ordenador con el exterior (Internet), avisándonos cuando se intenta hacer una comunicación no autorizada tanto desde dentro hacia fuera como a la inversa mostrándonos inclusive la IP del supuesto atacante.

Dentro de este tipo de programas nos encontramos con numerosas opciones por las que optar. Tenemos tanto firewalls de pago como gratuitos (freeware); dentro de los de pago tenemos Norton Internet Security 2003. En el sector de los gratuitos yo personalmente recomiendo dos (los cuales realmente son muy buenos y sobre todo teniendo en cuenta que son gratuitos) por un lado tenemos el ZoneAlarm y por otro el Tiny, no cabe duda de que a su vez hay numerosos programas, pero hay que ver si realmente nos están protegiendo de supuestos ataques.

No voy a decir donde conseguir estos programas que voy mencionando ya que evidentemente entiendo que sabéis manejar cualquier buscador; no obstante si alguien esta interesado en su traducción al Castellano o en algún manual para su configuración, que me manda un mail y prometo que intentaré responder a todos.

Encriptación.- Como hemos visto hasta el momento, llegamos a la convicción de que nuestra máquina no es tan segura como creíamos al principio; pues bien y ¿Qué podemos hacer para asegurar un poco más nuestro ordenador. Yo personalmente os recomiendo la encriptación y por supuesto también os recomiendo el programa scramdisk (http://scramdisk.clara.net). Este programa lo que hace es a grandes rasgos y muy resumido lo siguiente:

Crea un fichero (con un nombre que tu le pones y con un tamaño que tu le marcas) a simple vista aún dando con este fichero (que lo puedes guardar en cualquier carpeta) nadie sabrá de que programa es o con cual hay que abrirlo. Este fichero una vez activado nos resulta ser un Disco duro virtual con la capacidad que nosotros queramos y donde podemos almacenar ficheros, programas o lo que queramos, al cerrarlo se codifica y encripta de nuevo, siendo muy seguro si se configura correctamente. Aún suponiendo que dieran con el fichero y supiesen con que programa se tenía que arrancar, éste pide una contraseña (la cual utiliza unos logaritmos matemáticos muy complejos y muy buenos; solo cabe decir que de todos los logaritmos que presenta el programa, hasta la fecha solo uno ha conseguido ser violado) la cual evidentemente está encriptada.

Dada la importancia del programa así como su correcta configuración, el que esté interesado en el mismo y en su manual o instrucciones que me mande un mail.

Resumen de medidas de Seguridad a tomar.-

A continuación os pongo una relación de todas las medidas de seguridad que hemos tratado en este estudio, para que os sirva de guía a seguir en la forma de proteger vuestras máquinas.

- ∉ Instalar un Antivirus y procurar tenerlo actualizado.
- ∉ Instalación de un Firewall o cortafuegos.
- ∉ Instalar Windows en un directorio distinto que el que se marco por defecto.
- ∉ Visualizar extensiones de archivos.
- ∉ Cerrar puerto NetBios no compartiendo archivos (caso de ser necesario, poner contraseña a ese Puerto).
- ∉ Buena gestión de las contraseñas (cambio cada cierto tiempo, nombres raros nunca conocidos que puedan ser saltados un algún diccionario).
- ∉ Borrar las cookies cada cierto tiempo y por supuesto instalar el programa Ad-aware para el Spyware.
- ∉ Conocimiento total de los tipos de archivos (al objeto de no ejecutar ningún archivo ejecutable y que nos puedan meter algún troyano, virus, gusano, sploit, etc.
- ∉ Cuidadín con la Ingeniería Social (no seamos tan incrédulos).
- ∉ Instalación de un programa (repito: recomiendo el scramdisk) para la encriptación de nuestros datos más importantes y que no deben estar a la vista de la gente.

Todo lo aquí expuesto es a título educativo, yo no me responsabilizo si utilizáis esta información de forma no correcta o legal, siendo vosotros y solo vosotros los responsables de vuestros actos. Los ejemplos de hackeo que se mencionan y explican en este trabajo es simplemente eso, ejemplos; eso no quiere decir que tengáis que hacer lo mismo para alcanzar un nivel de seguridad en vuestras máquinas. Simplemente pienso que sabiendo como se puede atacar, uno puede defenderse mejor.

En caso de que observéis algún error o que yo mismo esté cometiendo algún fallo, ruego me lo comuniquéis mediante un e-mail al objeto de ser rápidamente subsanado.

Según el resultado, atención e interés que se muestre en este trabajo, actualizaré el mismo y lo iré poniendo según las nuevas novedades técnicas que vayan apareciendo, así como ampliaré el mismo y pondré diferentes manuales de configuración de programas aquí citados.

Tened cuidado ahí afuera.

jacktu2000@mixmail.com